REMARKS

Claims 1 to 13 are pending in the present application, claims 10 to 13 having been added herein. The office action and cited references has been considered. Favorable reconsideration is respectfully requested.

Claim 1 was objected to due to the extra line skip. Correction has been made.

Claim 6 was rejected under 35 USC § 101 as allegedly being directed to non-statutory subject matter. Without considering the merits of this rejection, Applicant has amended claim 6, to incorporate the subject matter regarding the hardware from claim 1. Withdrawal of this rejection is respectfully requested.

Claims 1, 5, 7 and 10 were rejected under 35 USC § 112, second paragraph. For the record, Applicant believes that the claims as original presented, considered in light of Applicant's specification (fully consistent with the law), would not have been confusing to those skilled in the art, and therefore the claims in their previous form are fully in accordance with §112. At **worst**, the claims including claim 1 in their previous form might be considered objectionable, but **only** as to form.

Nevertheless, in deference to the Examiner's views and to avoid or minimize needless argument, and as indicated above, a number of cosmetic amendments have been made in the claims. Such amendments are of a formal nature only, *i.e.*, made to place the claims in better form consistent with U.S. practice. These amendments are not "narrowing" amendments because the scope of the claims has not been reduced in these regards. No limitations have been added in these regards and none are intended.

Applicant notes with appreciation the indication of claim four is allowable over the prior art of record. Claims 1 through 3 were rejected under 35 USC § 102 (e) as being anticipated by Huttner ("Quantum Cryptography with Coherent States" and published by B. Huttner, N. Imoto, N. Gisin and T. Mor in Physical Review A 51, 1863 – 1869 (1995), hereinafter "Huttner"). This rejection is respectfully traversed the following reasons.

Claim 1 recites a method for exchanging a secure cryptographic key for a quantum cryptography apparatus employing non-ideal elementary quantum systems. The apparatus comprises an emitter and a receiver, being connected by a quantum channel and a conventional communication channel. The emitter encodes each bit at random onto a pair of non-orthogonal states belonging to at least two suitable sets, and there is not a single quantum operation reducing the overlap of the quantum states of all sets simultaneously. The emitter sends the encoded bit along the quantum channel to the receiver. The receiver randomly chooses an analysis measurement within said suitable sets. The emitter sends a set information along the conventional communication channel, and the receiver discards all received encoded bits for which he has chosen a different analysis measurement incompatible with the set they belonged to and sends an appropriate information to the emitter along the conventional communication channel. This is not taught, disclosed, or made obvious by the prior art of record.

The Huttner article consists of three parts. First, under the section entitled “Four-States Protocol”, it reviews the original BB84 quantum cryptography protocol, proposed by Charles Bennett and Gilles Brassard in 1984, and assesses its security. Second, the section entitled “Two-States Protocol” discusses the security of a second class of protocols, which use only two states and was first introduced by Charles Bennett in 1992. Finally, the authors propose a new class of protocols combining the advantages of the previous ones – the 4 + 2 Protocol.

Applicant will now discuss here why the protocol described in Claim 1 is clearly distinct from each of the three protocols of Huttner.

1) Four-State Protocol

The four-state protocol uses two sets of two states. In each set, one state codes for a “0” bit value and one for “1”. Moreover, the two states in a set are orthogonal. When photons are used and bits are encoded on polarization states, an example of suitable states is:

Set 1: Vertical = “0” and Horizontal = “1” polarization states

Set 2: Diagonal +45°=”0” and Diagonal –45° = “1” polarization states

2) Two-State Protocol

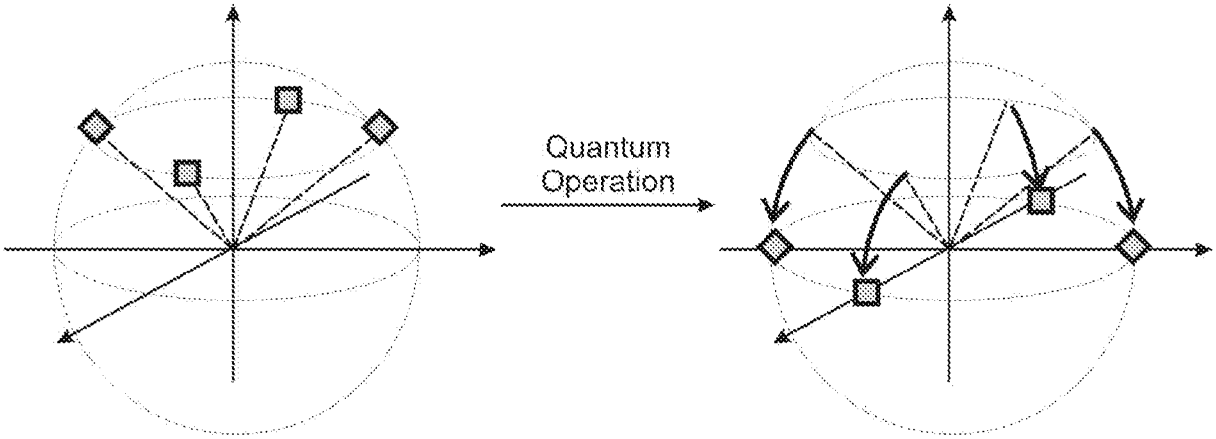
The two-state protocol is mentioned under III A of the paper. The two-state protocol uses one set of two states. These two states must be non-orthogonal. Moreover, it is essential for the security of this protocol to prevent an eavesdropper from simply removing some of the pulses. This can for example be achieved by the use of a strong reference pulse.

3) 4 + 2 Protocol

The 4 + 2 Protocol is a combination of the two previous protocols. It uses two sets of two states. In each set, one state codes for a "0" bit value and one for "1". Contrary to what is the case with the Four-State Protocol, the two states in one set are not orthogonal, which prevents an eavesdropper from deterministically distinguishing between the two states in each set.

However, there exists at least one quantum operation that can reduce the overlap of the quantum states of all set simultaneously. This is illustrated in the figure below, the left part of which is a reproduction of Figure 4 of Huttner. The right part of the figure shows that a quantum operation that reduces the vertical component of the states by a suitable amount would have the effect of making the states within a set orthogonal, *i.e.*, it reduces their overlap, and this for the two sets at the same time. After the operation, the states of one set are indeed located on opposite points of the Poincaré sphere, which implies that they are orthogonal. Consequently, it becomes possible for an eavesdropper to distinguish deterministically between the two states of one set.

Figure 4 of Huttner et al.



States used in the 4+2 protocol:

Set 1: ▨

Set 2: ◈

This general introduction to the three protocols shows the main differences between these protocols and Claim 1.

1) Four-State Protocol

Said first proposal, as well as the protocol of Applicant's claim 1, can be implemented using two sets of two states, but in contrast to the Four-State Protocol, the states in one set are not orthogonal: “the emitter encodes each bit at random onto a pair of non-orthogonal states belonging to at least two suitable sets”.

It is also important to note that the non-orthogonality of the states in a set is essential to the security of the protocol of Claim 1. This property ensures that an eavesdropper cannot distinguish deterministically between these two states after the sifting phase of the protocol. This is not the case in the Four-State Protocol and increases it vulnerability to an eavesdropper capable of implementing a so-called

"Photon Number Splitting Attack".

Therefore Claim 1 is not taught or suggested by the "Four-State Protocol" of Huttner.

2) Two-State protocol

The Examiner seems to mention the parts of the citation against claim 1 which relate to this protocol. The relevant parts are mentioned in the office action to be page 1865, lines 1-4. However, Applicant respectfully submits that the citation is not entirely correct. The protocol of Claim 1 requires at least *two sets of states* as mentioned in the claim and is thus clearly different from the Two-State protocol, which only uses one pair of non-orthogonal states belonging *to one suitable set of states*. Therefore the entire deduction on page 4 of the action is based on an erroneous assumption and therefore does not affect the patentability of claim 1. This is not only true for the initial point of one or two set of states but is equally true for the following passage, as *e.g.*, the portion of the rejection set forth on the last lines of page 4 referring to the entire left column of page 1865. Huttner only mentions one such set, therefore there is no choice to be made by the receiver between and "within said suitable set**s**". There is only one. Therefore Claim 1 is not taught or suggested by the "Two-State Protocol" of Huttner.

3) 4 + 2 Protocol

At the beginning of page 5 of the office action, the Examiner refers to page 1867, left column together with page 1865 left column (as cited above). This is a reference to this third protocol, from which description the drawing mentioned above was taken. However, the protocol of Claim 1 specifically calls for the use of states selected in such a way that there does not exist a single quantum operation reducing the overlap of the states in all sets simultaneously. This feature enhances the strength of this protocol versus the 4 + 2 Protocol. This property is illustrated in Figure 2 of the present application showing a similar procedure applied to the states shown on the left hand side of the drawing as shown in the above mentioned drawing. In other words, the application applies such an operation to the states in a similar diagram as it would be applied to the figure on page 1867 in Huttner. This figure shows that if the eavesdropper wants to reduce the overlap of the two states of one set (labelled set A on the figure) – or in other words to make them orthogonal so that they can be distinguished deterministically – he will at the same time reduce the overlap of the states of the second set (labelled set b) – and make them even less distinguishable. Therefore, this third protocol does not teach or suggest the protocol of the present claim 1.

According to the above mentioned analysis Applicant respectfully submits that the feature "not a single quantum operation reducing the overlap of the quantum states of all sets simultaneously" is clear and this feature can readily be understood upon reading the present specification in view of Fig. 2. Additionally, this feature is not taught or suggested by Huttner, nor obvious in view of Huttner, since someone skilled in the art would not be able to provide the distribution of the states according to the left hand side of Fig. 2 of the present application when starting from the figure on page 1867 in Huttner.

It is mentioned that the emitter encodes onto a pair of non-orthogonal states belonging to at least two suitable sets. It is then well defined for someone skilled in the art that these states are oriented in a way that there is not a single quantum operation reducing the overlap of the quantum states of *all sets simultaneously*,

For at least these reasons, Applicant respectfully submits that claim 1 is patentable over the prior art of record.

Claim 6 is amended to include limitations as in claim 1 to provide a coherent technical teaching to obtain a tangible result. Applicant respectfully submits that claim 6 is patentable over the prior art at least for the reasons discussed above with respect to claim 1. Additionally, Applicant respectfully submits that of the three protocols taught by Huttner, the one that most approaches the protocol of Claim 6 is the 4 + 2 protocol. The 4 + 2 protocol of Huttner also uses four non-orthogonal states. However, as illustrated in the figure used in the above explanation relating to Claim 1, the 4 + 2 protocol does not require that the states used are selected in such a way that it is not possible to find a single quantum operation, whether probabilistic or not, that reduces the overlap of the states of all sets simultaneously. This requirement, which is present in Claim 6, allows increasing the security of the protocol, by making it more difficult for an eavesdropper to obtain information about the states.

Claim 10 was rejected based on the Examiner's contention that Huttner teaches of a protocol, where the four states ¦+/-x> and ¦+/-y> are used by the emitter and the receiver randomly selects the σx or σy measurement. The Examiner is correct - this is also the case in the protocol described in Claim 10. Applicant respectfully submits, however that there are very important differences between the two protocols:

1) The convention used for bit value coding is completely different. For Huttner, a "0" bit value can be encoded by either of the two states ¦+x> and ¦+y>, whereas a "1" bit value is coded by either ¦-x> or ¦-y>.

Although the Pauli spin notation (¦[+/-] [x/y]>) is not explicitly used in Huttner, he teaches of the use of linear polarization states (vertical, horizontal and diagonal, Huttner, page 1864, "This protocol..."), which, as is well known to someone skilled in the art, can be equivalently described in terms of spins.

Note that in the class of protocols taught by Huttner, other conventions are possible, as long as the two states that code for the same bit value are not orthogonal (*e.g.*, ¦+x> and ¦+y>).

In Claim 10, a "0" bit value is coded on ¦+/-x> and a "1" on ¦+/-y>. It is thus clear that contrary to what Huttner teaches, a bit value is coded on one of two orthogonal states (¦+x> and ¦-x> for "0" for example).

2) In the protocol taught by Huttner, after having sent at least one quantum state to the receiver, the emitter announces for the corresponding states whether it belonged to the x set (¦+/-x>) or the y set (¦+/-y>). This phase is also known as the "sifting" phase. Assuming, for example, that ¦+x> was transmitted, the emitter announces ¦+/-x>, *i.e.*, a pair of orthogonal states, which includes the one it sent.

In the protocol of Claim 10, after the transmission phase, the emitter also announces a pair of states. In this case however, it announces a pair of non-orthogonal states, which includes the one it sent. Assuming, for example, that it sent a ¦+x> state, it will announce {¦+x>;¦+y>} with 50% probability and {¦+x>;¦-y>} with 50% probability.

In summary, the state announcement phase of the two protocols has two very important differences:

- announcement of a pair of orthogonal (Huttner) or of a pair of non-orthogonal states (Claim 10)
- deterministic announcement in Huttner (this means that if a given state is transmitted, the emitter always announces the same pair) vs. probabilistic announcement in Claim 10.

The differences listed above clearly indicate that the protocol described in Claim 10 is not taught in Huttner.

For at least these reasons, Applicant respectfully submits the claim 10 is patentable over the prior art of record. Claims 2 through 5, 7 through 9 and 11 through 13 are believed to be patentable at least for the reasons discussed above with respect to claims 1, 6 and 10.

In view of the above amendments and remarks, Applicant respectfully submits that claims 1 through 13 are patentable over the prior art of record. Applicant submits that the application is in condition for allowance. Early notice to this effect is most earnestly solicited.

If the Examiner has any questions he is invited to contact the undersigned to advance prosecution.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant(s)

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:me
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\bn\i\isle\gisin1a\pto\2007-03-05amendmnet.doc